REMARKS

The Examiner has again rejected Claims 1-22 under 35 U.S.C. §102(e) as allegedly being anticipated by Segal (6,345,299). Applicant respectfully disagrees with such rejection, since the Examiner's sole reference still fails to meet each of applicant's independent claim limitations. Moreover, the Examiner has not even considered applicant's arguments regarding the pending dependent claims.

In the Examiner's response to Amendment A, the Examiner continues to rely on the following excerpt from Segal to make a prior art showing of applicant's claimed "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" (see Claims 1 and 17), "maintaining a set of scanning rules for determining when a communication received at a firewall is to be scanned on the firewall and when said communication may be scanned by the destination node of said communication" (see Claim 7), "a set of criteria to be applied to said communication to determine if said communication is to be scanned for target content at the firewall or at the destination node" (see Claim 18), and "a set of rules configured to determine whether said communication is to be scanned for said target content on said firewall or on the first node" (see Claim 19).

> "In accordance with the invention, the network 40 the units 43, 45, 46, 47, 49, and 50 each comprise a shared list setting forth a plurality of listed nodes and a set of access privileges for each listed node. Access privileges are the types of transmissions that a given node listed in the shared list is permitted to make. For example, consider the case where node B1 is a computer or LAN at an accounting firm. The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed

> nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 2, line 60 - col. 3, line 15)

Specifically, with respect to applicant's claimed "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" (emphasis added), the Examiner points out the foregoing discussion of the exemplary use of the shared list in Segal, and then concludes "Segal discloses that the node and the firewall communicate to determine which transmissions are to be transmitted."

Even if the Examiner conclusion summary accurately describes what Segal discloses, it still fails to meet all of applicant's claim limitations. In the Examiner's cited example above, the node B1 is not capable of any scanning, thus there is clearly no disclosure, teaching or even suggestion of any sort of determining when one of said communications **may be scanned at a computer node** connected to the firewall **instead of at the firewall**. Only applicant's teaches and claims such specific interplay between a computer node and a firewall, whereby scanning occurs on one or the other based on a set of criteria.

The Examiner continues by stating that Segal inherently discloses a virus scanner, in view of the excerpt from Segal below:

> "The situation can be improved upon by providing a set of firewall-type commands that include lists of which nodes, sources, networks are allowed to use certain destinations. These commands can be utilized by filtering devices and/or security devices such as firewalls, ingress nodes, switches, which would be informed which destination nodes, addresses, ports, are permitted to which source nodes or networks. These filtering devices and/or security devices may be separate stand-alone components or their capability may be integrated into other, possibly already existing, devices." (col. 3, lines 35-45)

The Examiner continues by concluding that "Segal discloses a firewall that filters and scans data." First, applicant notes that there is no mention of "scanning" in Segal. Moreover, even if there were some sort of scanning inherently disclosed in Segal, it would still fail to meet applicant's claimed "virus scanner" feature.

Applicant asserts that the disclosure of a firewall does not necessarily meet the limitation of a "virus scanner." neither explicitly or implicitly. See, for example, an illustrative definition of a firewall, indicating the broadest plain and ordinary meaning thereof.

> "firewall
>
> A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
> There are several types of firewall techniques:
>
> Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
> Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
> Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
> Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.
> In practice, many firewalls use two or more of these techniques in concert.
>
> A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted." http://www.webopedia.com/TERM/f/firewall.html

There is simply no mention of any sort of virus scanning in such definition. Applicant further brings the Examiner's attention to what is well known in the computer industry, namely virus scanner and firewall products/features are separate entities which, may be used in combination, but are nevertheless functionally different. Again, the Segal reference fails to meet applicant's claims.

It is further noted that the Examiner's reference does not adequately meet the limitations of applicant's dependent claims. It thus appears that applicant's dependently claimed subject matter has not been fully considered by the Examiner. Just by way of example, the Examiner relies on the foregoing excerpts from Segal to make a prior art showing of applicant's claimed:

> "wherein said partitioning comprises:
>
> receiving scanning capabilities of a first computer node connected to the firewall;
>
> consulting a set of scanning requirements specified by an operator of the firewall; and
>
> specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node" (see Claim 4), and
>
> "wherein said determining comprises:
>
> identifying whether said firewall is capable of scanning said first communication for target content;
>
> determining whether said firewall is configured to share responsibility for scanning said communications with one or more of said plurality of computer nodes;
>
> determining whether said first node is capable of scanning said first communication for said target content; and
>
> determining whether said communication satisfies one or more criteria in said set of criteria" (see Claim 6).

Similar to the independently claimed subject matter, this functionality is clearly absent in Segal. A specific prior art showing of such features or a notice of allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P263/99.010.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172
Telephone: (408) 505-5100